No matter if you do an internal, external, AD or even web application test you might need to generate password lists in order to try some brute forcing.

### Create wordlist from website

This can be done with wordlist-extractor in burp.

## Create wordlist from Active Directory

This oneliner will get the Firstname (givenName), Lastname (sn) and Firstname and Lastname combinend (name) of a user, and the name of all the computers. Remove whitespace, and turn them all into lowercase and remove duplicates.

Of course you will need to change the `-h` flag to the correct domain-controller ip/hostname, change `-b` flag to the correct domain name, and `-D` to the Distinguished name of your user, and the `-w` to your users password.

```
ldapsearch -h evilcorp.local  -w SecretPassword  -b "dc=evilcorp,dc=local" -D "cn=Philip L,cn=users,dc=evilcorp,dc=local" "(|(object
```